What is claimed is:

1. A method comprising:

generating at least one descriptor in a pre-boot environment associated with establishing a protection policy for at least one firmware resource;

storing the at least one descriptor in a resource protection list; and

storing the resource protection list in a location accessible in a post-boot environment.

2. A method as defined in claim 1, further comprising initializing the at least one firmware resource in the pre-boot environment.

3. A method as defined in claim 1, further comprising generating at least one hash code based on the at least one descriptor.

4. A method as defined in claim 3, further comprising storing the at least one hash code in a trusted protection module platform configuration register.

5. A method as defined in claim 1, further comprising storing the at least one descriptor in an advanced configuration and power interface differentiated system descriptor table.

6. A method as defined in claim 1, wherein the at least one firmware resource includes at least one of a register region, a firmware data memory region, a firmware code memory region, and a hand-off information memory region.

7. A method as defined in claim 1, wherein the pre-boot environment comprises executing at least one of a basic input output system and an extensible firmware interface.

8. A method as defined in claim 1, wherein storing the resource protection list comprises storing the resource protection list in a location accessible by at least one of a secure virtual machine monitor and an operating system in the post-boot environment.

9. A method as defined in claim 1, further comprising establishing a resource protection policy in the post-boot environment based on the resource protection list.

10. A method as defined in claim 1, further comprising enabling the resource protection list to be validated in the post-boot environment.

11.   An apparatus comprising:

a processor system; and

a memory communicatively coupled to the processor system, the

memory including stored instructions that enable the processor system to:

generate at least one descriptor in a pre-boot environment

associated with establishing a protection policy for at least one

firmware resource,

store the at least one descriptor in a resource protection list, and

store the resource protection list in a location accessible in a

post-boot environment.

12.   An apparatus as defined in claim 11, wherein the instructions stored in

the memory enable the processor system to initialize the at least one firmware

resource in the pre-boot environment.

13.   An apparatus as defined in claim 11, wherein the instructions stored in

the memory enable the processor system to generate at least one hash code based on

the at least one descriptor.

14.   An apparatus as defined in claim 13, wherein the instructions stored in

the memory enable the processor system to store the at least one hash code in a trusted

protection module platform configuration register.

15.   An apparatus as defined in claim 11, wherein the instructions stored in the memory enable the processor system to store the at least one descriptor in an advanced configuration and power interface differentiated system descriptor table.

16.   An apparatus as defined in claim 11, wherein the at least one firmware resource includes at least one of a register region, a firmware data memory region, a firmware code memory region, and a hand-off information memory region.

17.   An apparatus as defined in claim 11, wherein the instructions stored in the memory enable the processor system to execute at least one of a basic input output system and an extensible firmware interface in the pre-boot environment.

18.   An apparatus as defined in claim 11, wherein the instructions stored in the memory enable the processor system to store the resource protection list in a location accessible by a secure virtual machine monitor in the post-boot environment.

19.   An apparatus as defined in claim 11, wherein the instructions stored in the memory enable the processor system to enable the resource protection list to be validated in the post-boot environment.

20.   An apparatus as defined in claim 11, wherein the instructions stored in the memory enable the processor system to establish a resource protection policy in the post-boot environment based on the resource protection list.

21.   A computer readable medium having instructions stored thereon that, when executed, cause a machine to:

generate at least one descriptor in a pre-boot environment associated with establishing a protection policy for at least one firmware resource;

store the at least one descriptor in a resource protection list; and

store the resource protection list in a location accessible in a post-boot environment.

22.   A computer readable medium as defined in claim 21 having instructions stored thereon that, when executed, cause the machine to initialize the at least one firmware resource in the pre-boot environment.

23.   A computer readable medium as defined in claim 21 having instructions stored thereon that, when executed, cause the machine to generate the at least one descriptor for at least one of a register region, a firmware data memory region, a firmware code memory region, and a hand-off information memory region.

24.   A computer readable medium as defined in claim 21 having instructions stored thereon that, when executed, cause the machine to generate at least one hash code based on the at least one descriptor.

25.   A computer readable medium as defined in claim 24 having instructions stored thereon that, when executed, cause the machine to store the at least one hash code in a trusted protection module platform configuration register.

26.   A computer readable medium as defined in claim 21 having

instructions stored thereon that, when executed, cause the machine to store the at least

one descriptor in an advanced configuration and power interface differentiated system

descriptor table.

27.   A computer readable medium as defined in claim 21 having

instructions stored thereon that, when executed, cause the machine to execute at least

one of a basic input output system and an extensible firmware interface in the pre-

boot environment.

28.   A computer readable medium as defined in claim 21 having

instructions stored thereon that, when executed, cause the machine to store the

resource protection list in a location accessible by a secure virtual machine monitor in

the post-boot environment.

29.   A computer readable medium as defined in claim 21 having

instructions stored thereon that, when executed, cause the machine to enable the

resource protection list to be validated in the post-boot environment.

30.   A computer readable medium as defined in claim 21 having

instructions stored thereon that, when executed, cause the machine to establish a

protection policy in the post-boot environment based on the resource protection list.

31.   An apparatus comprising:

a processor system; and

a flash memory communicatively coupled to the processor system, the flash memory including stored instructions that enable the processor system to:

generate at least one descriptor in a pre-boot environment associated with establishing a protection policy for at least one firmware resource,

store the at least one descriptor in a resource protection list, and

store the resource protection list in a location accessible in a post-boot environment.

32.   An apparatus as defined in claim 31, wherein the at least one firmware resource includes at least one of a register area, a firmware data memory region, a firmware code memory region, and a hand-off information memory region.